Lisa Weintraub Schifferle (DC Bar No. 463928)
Kristin Krause Cohen (DC Bar No. 485946)
Kevin H. Moriarty (DC Bar No. 975904)
Katherine E. McCarron (DC Bar No. 486335)
John A. Krebs (MA Bar No. 633535)
Andrea V. Arias (DC Bar No. 1004270)
Jonathan E. Zimmerman (MA Bar. No. 654255)
Federal Trade Commission
600 Pennsylvania Ave., NW Mail Stop NJ-8100
Washington, D.C. 20580
Telephone: (202) 326-2252
lschifferle@ftc.gov
kcohen@ftc.gov
kmoriarty@ftc.gov
kmccarron@ftc.gov
jkrebs@ftc.gov
aarias@ftc.gov
jzimmerman@ftc.gov

Attorneys for Plaintiff Federal Trade Commission

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. Wyndham Worldwide Corporation, *et al.*, Defendants.	Case No. 2:12-cv-01365-PHX-PGR **PLAINTIFF'S RESPONSE IN OPPOSITION TO WYNDHAM HOTELS AND RESORTS' MOTION TO DISMISS**

INTRODUCTION

The Federal Trade Commission ("FTC") opposes the motion by Wyndham Hotels and Resorts, LLC ("Hotels and Resorts"), joined by Wyndham Worldwide Corporation ("Wyndham Worldwide"), Wyndham Hotel Group, LLC ("Hotel Group"), and Wyndham Hotel Management ("Hotel Management") (collectively, "Wyndham" or "Defendants"), to dismiss this action pursuant to Federal Rule of Civil Procedure 12(b)(6) ("Wyndham Mot."). (ECF No. 32.) In its motion, Wyndham abandons any pretense of meeting the 12(b)(6) standard and, instead, uses its brief as a platform to advance meritless theories attacking the FTC's longstanding use of the authority granted to it by Congress to protect consumers against unfair and deceptive practices. These arguments should be rejected by the Court.

FACTUAL BACKGROUND

On June 26, 2012, the FTC filed a two-count complaint against the Defendants under Section 13(b) of the Federal Trade Commission Act ("FTC Act"). *See* 15 U.S.C. § 53(b). The FTC subsequently amended its complaint on August 8, 2012 (the "Complaint"). (ECF No. 28.) The Complaint alleges that Defendants violated the FTC Act in connection with their failure to employ reasonable data security practices, which resulted in three data security breaches in less than two years, the known theft of hundreds of thousands of consumers' payment card account numbers, and millions of dollars in fraud loss. (Compl. ¶¶ 1-2.)

The Complaint specifically alleges a number of security failures, including: failing to limit access among different computer networks through the use of readily available measures, such as firewalls (*id.* at ¶ 24(a)); failing to configure software properly to prevent the storage of payment card information in clear text (*id.* at ¶ 24(b)); failing to ensure the Wyndham-branded hotels had adequate information security policies in place prior to allowing them to access Wyndham's computer network (*id.* at ¶ 24(c)); failing to require servers attached to its networks to have the latest security patches from manufacturers (*id.* at ¶ 24(d)); failing to change commonly-known default passwords

within its network (*id.* at ¶ 24(e)); failing to follow best practices for password complexity (*id.* at ¶ 24(f)); failing to inventory the computers on its network in order to permit Wyndham to identify the origin of intrusion efforts (*id.* at ¶ 24(g)); failing to employ reasonable measures to detect and prevent unauthorized access (*id.* at ¶ 24(h)); failing to follow proper procedures to prevent repeated intrusions (*id.* at ¶ 24(i)); and failing to restrict third-party access to its network (*id.* at ¶ 24(j)).[1]

The Complaint alleges that these failures resulted in two violations of the FTC Act. The first count alleges that Wyndham engaged in deceptive business practices in violation of Section 5 of the FTC Act by misrepresenting the security measures it undertook to protect consumers' personal information. (*id.* at ¶¶ 44-46.) The second count alleges that Wyndham's failure to provide reasonable data security is an unfair trade practice, also in violation of Section 5 of the FTC Act. (*id.* at ¶¶ 47-49.) Specifically, the Complaint alleges that Wyndham engaged in unfair business practices because its failure to use reasonable methods to safeguard consumers' personal information caused or is likely to cause substantial injury that could not be avoided by consumers and was not outweighed by countervailing benefits. (*Id.*)

In response to the FTC's Complaint, Wyndham filed two motions to dismiss. This opposition addresses the motion filed by Hotels and Resorts, challenging the FTC's authority to bring the unfairness count under the FTC Act and arguing that the deception count fails to state a claim.

ARGUMENT

Section 5 of the FTC Act prohibits unfair or deceptive practices, and the Complaint pleads sufficient facts to allege that Defendants engaged in unfair and deceptive practices as a result of their failure to maintain reasonable and appropriate data security and their misrepresentations to consumers about the quality of their data security.

[1] Wyndham repeatedly denies the existence of these highly specific allegations. (Wyndham Mot. 3, 10, 14.) A simple reading of the Complaint demonstrates that these denials are meritless.

I. LEGAL STANDARD.

Wyndham's motion to dismiss is brought pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. A Rule 12(b)(6) motion tests the sufficiency of a complaint's allegations. *United States v. Corinthian Colleges*, 655 F.3d 984, 991 (9th Cir. 2011). To survive such a motion, the plaintiff need only allege facts sufficient to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 554, 570 (2007)). Facial plausibility is established where the plaintiff "pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. In reviewing a Rule 12(b)(6) motion to dismiss for failure to state a claim, a court will "accept as true all facts alleged in the complaint, and . . . draw all reasonable inferences in favor of [the plaintiff.]" *Newcal Indus., Inc. v. Ikon Office Solution*, 513 F.3d 1038, 1043 n.2 (9th Cir. 2008). Under this standard, the Complaint states a claim for relief and Wyndham's motion to dismiss must be denied.

II. THE COMPLAINT SATISFIES THE PLEADING STANDARD FOR UNFAIRNESS.

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). To state a claim for unfairness under the FTC Act, the FTC must plead that an act or practice caused or is likely to cause substantial injury to consumers, that the injury was not reasonably avoidable by consumers, and was not outweighed by countervailing benefits. 15 U.S.C. § 45(n); *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1153 (9th Cir. 2010). Wyndham offers no serious argument that the FTC has not done so.[2]

[2] Wyndham incorrectly identifies unfairness as requiring "unconscionable or oppressive" acts (Wyndham Mot. 1-2), a standard that Congress has specifically rejected. Nearly fifty years ago, the FTC promulgated a rule stating that one factor to determine unfairness was whether the act or practice was "immoral, unethical, oppressive, or unscrupulous." Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking. 29 Fed. Reg. 8355 (July 2, 1964). Congress codified unfairness, as stated above, and neither that codification nor applicable precedent includes the "unconscionable and oppressive"

As described above, the Complaint identifies, with specificity, ten data security failures that unreasonably and unnecessarily exposed consumers' personal data to unauthorized access. (Compl. ¶ 24(a)-(j).) These allegations include, among other things, data security failures related to firewalls, storing sensitive data unencrypted and without a business need, security patches, and password policies; and, as alleged, are more than satisfactory to comply with the "short and plain statement" requirement of Rule 8(a)(2). Fed. R. Civ. P. 8(a)(2). The Complaint also alleges that these practices caused substantial injury (*e.g.*, Compl. ¶ 40), which was not reasonably avoidable (*e.g.*, *id.* at ¶¶ 40, 48), and which was not outweighed by countervailing benefits (*e.g.*, *id.* at ¶ 48).

Rule 8 does not require the "hyper-technical" pleading that Wyndham appears to demand in its motion. *Iqbal*, 556 U.S. at 678. The Complaint provides more than enough "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.*

III. THE FTC HAS THE AUTHORITY TO ENFORCE THE FTC ACT AGAINST ENTITIES FOR UNFAIR PRACTICES RELATED TO DATA SECURITY.

As explained above in Part II, the Complaint satisfies the pleading standard for unfair practices. This should end the inquiry. The purpose of this Part is to rebut Wyndham's meritless arguments that (a) the FTC lacks authority to pursue an unfair practices claim related to data security, (b) that unfairness actions related to data security require rulemaking, and (c) insufficient injury results from a payment card breach.

A. FTC Unfairness Authority Does Not Exclude Data Security

Instead of arguing that the FTC does not state a claim of unfair practices, Wyndham argues that applying unfairness to data security practices somehow would be inconsistent with the statutory scheme. (Wyndham Mot. 6.) Wyndham does not dispute that its business practices are "in or affecting commerce," 15 U.S.C. § 45(a)(1), that it is a

---

standard that Wyndham reads into the statute. FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691 (1994) (codified at 15 U.S.C. § 45(n)).

"person, partnership, or corporation," *id*., and that none of the express sector-specific exemptions in Section 5 applies, *see id*. § 45. Rather, Wyndham reads into the FTC Act an inexplicable exemption for data security that appears nowhere in the text.

Wyndham's position lacks any statutory or precedential support. The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce, limited only by sector-specific statutory exclusions, none of which applies to Wyndham. The FTC has consistently applied its authority to data security practices, bringing forty-one enforcement actions in this area. Congress has confirmed the FTC's authority implicitly and explicitly.

1. Section 5 of the FTC Act Gives the FTC Enforcement Authority over Unfair Practices that Satisfy § 45(n).

Congress purposefully delegated broad power to the FTC under Section 5 of the FTC Act to address unanticipated practices in a changing economy. *See FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1194 (10th Cir. 2009) ("[T]he FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws."). The legislative history of the FTC Act reflects Congress's concerns about attempting to enumerate specific acts and practices. S. Rep. No. 63-597, at 13 (1914) ("there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others"); H.R. Rep. No. 63-1142, at 19 (1914) (Conf. Rep.) ("It is impossible to frame definitions which embrace all unfair practices."). As a result of these concerns, in drafting an analogous FTC Act provision, Congress "rejected[] the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (citing S. Rep. No. 63-597, at 13 (1914)).

Contrary to Wyndham's alarmism, the absence of enumerated unfair practices does not mean that the FTC can "regulate anything and everything." (Wyndham Mot. 6.) The FTC's Section 5 authority over "unfair or deceptive acts or practices in or affecting

commerce" is proscribed by the nature of the alleged injury to the consumer. *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985) ("[T]he consumer injury test is the most precise definition of unfairness articulated by either the Commission or Congress."). The elements of unfairness were codified in 1994:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

15 U.S.C. § 45(n).[3] As described in Part II, the Complaint alleges facts to support precisely this injury. Wyndham does not and cannot provide any reason why the instrumentality of its unfair practice—unreasonable data security—somehow exempts it from the FTC's well-established unfairness authority.

Wyndham's criticism that data security is not enumerated in the "plain text of Section 5" (Wyndham Mot. 6) simply states the obvious: Section 5 does not identify specific acts or practices. Indeed, the statute also does not mention *any* of the established uses of its unfairness provision, including unsafe farm equipment (*see In the Matter of Int'l Harvester Company*, 104 F.T.C. 949 (1984)); online check drafting and delivery (*see Neovi*, 604 F.3d 1150); business opportunity scams (*see FTC v. Stefanchik*, 559 F.3d 924 (9th Cir. 2010)); weight-loss products (*see FTC v. Garvey*, 383 F.3d 891 (9th Cir. 2004)); telephone billing processors (*FTC v. Inc21.com Corp.*, 2012 WL 1065543, No. 11-15330 (9th Cir. March 30, 2012)); or many other practices affecting commerce, all of which courts routinely find to be subject to Section 5 of the FTC Act. Congress clearly intended the FTC Act to give the FTC the broad enforcement authority that Wyndham asks the Court to read out of the statute.

---

[3] There are other limits as to Section 5 generally, but only as to particular industries, not specific practices. 15 U.S.C. § 45(a)(2) ("The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions[,] Federal credit unions[,] common carriers[,] air carriers and foreign air carriers[,] and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act[.]"). None of the statutory exceptions applies here.

2. The FTC Has Always Affirmed, and Never Disavowed, Authority Over Unfair Practices Related to Data Security.

Wyndham argues that the FTC originally disclaimed authority to pursue unfair practices related to data security and that its position in this matter is a "quite recent[]" reversal. (Wyndham Mot. 6-7.) These claims are contrary to fact: Since 2000, the FTC has brought forty-one data security cases. *See* Legal Resources | BCP Business Center, http://business.ftc.gov/legal-resources/29/35. Thirty-six of those cases were brought under the FTC Act, and seventeen alleged unfair practices. *Id*. The FTC has routinely reported and publicized its data security program, including these enforcement activities, to Congress, consumers, and industry. *See*, *e.g.*, Identity Theft: Innovative Solutions for an Evolving Problem: Hearing before the Subcomm. on Terrorism, Technology, and Homeland Security of the S. Comm. on the Judiciary 110th Cong. (March 21, 2007) (Prepared Statement of the Federal Trade Commission) ("[I]n several of the cases, the alleged security inadequacies led to breaches that caused substantial consumer injury and were challenged as unfair practices under the FTC Act.").[4]

Wyndham incorrectly asserts that the FTC disclaimed its authority when it stated that it "lacks authority to require firms to adopt information practice policies." (Wyndham Mot. 7 (quoting FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 33-34 (May 2000) *available* at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf ("Privacy Report")).) Wyndham mischaracterizes the Privacy Report, which states only that FTC Act authority under Section 5 is limited to unfair or deceptive practices, and thus would not encompass failure to adopt certain policies *absent* unfair or deceptive practices. The same Privacy Report explicitly states, in a section titled "Current FTC Authority," that "[t]he FTC Act

[4] The FTC has reported to Congress *more than thirty times* since 2003 on its Section 5 enforcement activities related to data security. *See*, *e.g.*, Identity Theft: Hearing before the H. Comm. on Financial Services 108th Cong. (April 3, 2003) (Prepared Statement of the Federal Trade Commission); Data Security: Hearing before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade 112th Cong. (June 15, 2011) (Prepared Statement of the Federal Trade Commission).

prohibits unfair and deceptive practices in and affecting commerce. It authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and *provides a basis for government enforcement of certain fair information practices*." *Id*. at 33-34 (emphasis added). Moreover, even if the FTC had originally disavowed its authority, which it did not, that fact would not be controlling. *See Smiley v. Citibank*, 517 U.S. 735, 742 (1996) ("[T]he mere fact that an agency interpretation contradicts a prior agency position is not fatal.").

3. Data Security Statutes Do Not Limit FTC Authority Under the FTC Act.

Wyndham argues that several statutes that provide the FTC with legal tools to address data security in specific contexts somehow "preclude" or "foreclose" an interpretation of the FTC Act to cover unfair and deceptive acts or practices related to data security. (Wyndham Mot. 7-8 (citing *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000)).) But Wyndham has not argued (nor could it) that there is a contradiction that requires reconciliation between the FTC Act and other data security statutes. *Cf. Brown & Williamson*, 529 U.S. at 139 (finding FDA's interpretation to "plainly contradict congressional policy"). For example, the Fair Credit Reporting Act ("FCRA"), Gramm-Leach-Bliley Act ("GLB"), and Children's Online Privacy Protection Act ("COPPA") neither expressly nor impliedly restrict FTC Act authority over unfair practices related to data security. Rather, they enhance the FTC's legal tools beyond the FTC Act by giving the FTC either civil penalty or rulemaking authority in specific circumstances.[5] Nothing in the FCRA, GLB, and COPPA can be viewed as an effort to restrict or deny the existence of FTC authority over unfair or deceptive acts or practices related to data security, nor is the existence of these statutes inconsistent with the FTC's

[5] In the case of the FCRA and COPPA, the statutes give the FTC, among other things, authority to impose civil penalties for certain unreasonable data security practices by credit reporting agencies and for those related to children, respectively. *See* 15 U.S.C. § 1681, *et seq.* (FCRA) and 15 U.S.C. § 6501-6506 (COPPA). In the case of GLB, the statute gives the FTC rulemaking authority with regard to financial institutions. 15 U.S.C. §§ 6801-6809.

continuing authority to pursue unfair data security practices under the FTC Act.[6]

Moreover, Wyndham's admission that "the FCRA, GLBA, and COPPA, grant the FTC authority to regulate data-security standards" (Wyndham Mot. 8) undermines its argument that it is not "conceivable that Congress, through implication, would have delegated the task of mandating affirmative data-security requirements to the FTC—an agency that has no particular expertise in either the policy or technology of data-security issues." (*Id*. at 9). That Congress *has* delegated data security authority to the FTC belies Wyndham's claim that Congress never would have done so because of a lack of expertise.[7] Indeed, when Congress recently created the Consumer Financial Protection Bureau ("CFPB"), it transferred the majority of GLB and FCRA rulemaking authority to the CFPB, but not rulemaking authority related to data security. 12 U.S.C. § 5481(12)(J) (excluding certain provisions of the FCRA and GLB).

4. Congressional Interest in Data Security Neither Impliedly Nor Explicitly Deprives the FTC of its FTC Act Authority over Unfair and Deceptive Data Security Practices.

Nor is there any authority for Wyndham's argument that the "intense debate among members of Congress" could, by inference, somehow strip the FTC of its established authority under the FTC Act over unfair practices. (Wyndham Mot. 8-9.) Wyndham argues that Congressional interest in data security, and its failed efforts to pass specific data security legislation, create the presumption that "Congress could not have intended to delegate" data security authority to the FTC under the FTC Act. (Wyndham Mot. 8-9 (quoting *Brown & Williamson*, 529 U.S. at 160).) This argument is contrary to fact and precedent.

---

[6] To the extent that Wyndham is arguing that these laws impliedly repeal the scope of the FTC Act, it has failed to meet that standard. *See Nat'l Ass'n of Home Builders v. Defenders of Wildlife*, 551 U.S. 644, 662-63 (2007) (implied repeals are disfavored).

[7] Wyndham's expertise argument also is undermined by its acknowledgment of the FTC's authority to pursue data security practices pursuant to the deception provision of Section 5. (Wyndham Mot. 1.) If the FTC is equipped to evaluate the deceptiveness of Wyndham's claims of "industry standard" and "commercially reasonable" data security (Compl. ¶ 21), then it is equipped to determine whether Wyndham lacked reasonable and appropriate data security, as alleged under the unfairness count.

If relevant at all, the facts of the congressional debate over data security affirm FTC authority over unfair practices related to data security. For example, of the six data security bills Wyndham cites in support of its argument, four included savings clauses to *preserve the FTC's existing data security authority*. *See* S. 1207 § 6(d), 112th Cong. (1st Sess. 2011); H.R. 2577 § 6(d), 112 Cong. (1st Sess. 2011); H.R. 1841 § 6(d), 112 Cong. (1st Sess. 2011); H.R. 1707 § 6(d), 112 Cong. (1st Sess. 2011). Preservation clauses would be unnecessary if the FTC lacked any existing authority. Similarly, Senator Rockefeller, who co-sponsored Senate Bill 1207, asked an FTC representative: "Can you talk about how Senator Pryor's and my bill will *complement your existing enforcement efforts*?" Privacy and Data Security: Protecting Consumers in the Modern World: Hearing on S.B. 1207 before the S. Comm. on Commerce, Science, and Transportation (June 29, 2011) at 32 (emphasis added). Thus, as a factual matter, there is no support for Wyndham's argument that Congress is implying that it believes the FTC lacks authority.

Moreover, accepting Wyndham's premise that Congress is engaged in an "intense debate" over data security, precedent establishes that congressional inaction affirms the FTC's interpretation of the scope of the FTC Act. *United States v. Rutherford*, 442 U.S. 544, 553-54 (1979) (citations omitted) ("[D]eference is particularly appropriate where, as here, an agency's interpretation involves issues of considerable public controversy, and Congress has not acted to correct any misperception of its statutory objectives."). Deference also is appropriate where, as here, Congress, after being informed of the agency's interpretation, has amended a statute (*e.g.*, U.S. SAFE WEB Act of 2006, PL 109–455, December 22, 2006, 120 Stat 3372), but not taken any steps to limit the contested interpretation. *See Saxbe v. Bustos*, 419 U.S. 65, 74 (1974) ("This longstanding administrative construction is entitled to great weight, particularly when, as here, Congress has revisited the Act and left the practice untouched."); *Bunker Hill Co. v. EPA*, 658 F.2d 1280, 1284 n.2 (9th Cir. 1981) ("[A]n administrative interpretation deserves particular deference where Congress fails to take advantage of an opportunity to alter it."). Thus, Congress's inaction regarding the FTC's longstanding and widely-reported

authority over unfair practices related to data security confirms this authority.

5. Wyndham's Reliance on Brown & Williamson is Misplaced.

Wyndham relies almost exclusively on *Brown & Williamson* for its argument that Wyndham's unreasonable data security cannot be an unfair practice under Section 5. This reliance is misplaced. The FTC's longstanding data security program has none of the hallmarks of the FDA's assertion of authority over tobacco that was rejected in *Brown & Williamson*. In *Brown & Williamson*, Congress had created a tobacco regulatory regime in response to the FDA's "representations to Congress *since 1914*," that the FDA lacked authority to regulate tobacco. *Brown & Williamson*, 529 U.S. at 159 (emphasis added). The FDA's subsequent assertion of authority regarding tobacco "would require the agency to ban" tobacco products under the FDCA, a result that would have mooted the congressionally-authorized regulatory regime. *Id*. at 137 ("Congress, however, has foreclosed the removal of tobacco products from the market."). As a result, it was necessary for the Court to undertake the "task of reconciling many laws enacted over time, and getting them to 'make sense' in combination." *Id*. at 143 (citing *United States v. Fausto*, 484 U.S. 439, 453 (1988)). These were the "extraordinary" circumstances that led the Court to overturn the FDA's assertion of authority. *Id*. at 159-60. By contrast, the FTC has never disclaimed authority over unfair and deceptive data security practices, and Congress has enacted no legislation that is inconsistent or irreconcilable with the FTC's authority over data security practices pursuant to the FTC Act. The FTC's interpretation of Section 5 to cover unfair data security practices is therefore proper.

B. The FTC Is Not Required to Address Data Security Through Rulemaking.

Wyndham also argues that it is inappropriate to address data security in an enforcement action and, instead, the FTC must first set forth guidelines through rulemaking. (Wyndham Mot. 10-11 (citing *Ford Motor Co. v. FTC*, 673 F.2d 1008, 1010 (9th Cir. 1981); *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 294 (1974)).) As a preliminary matter, and as Wyndham concedes, both the Ninth Circuit in *Ford Motor* and

the Supreme Court in *Bell Aerospace* acknowledge that an agency "is not precluded from announcing new principles in the adjudicative proceeding . . . ." *Ford Motor*, 673 F.2d at 1009 (quoting *Bell Aerospace*, 416 U.S. at 294). The decision of whether to proceed through case-by-case enforcement or rulemaking is left to the "informed discretion of the administrative agency." *San Luis Obispo Mothers for Peace v. Nuclear Regulatory Comm'n*, 449 F.3d 1016, 1027 (9th Cir. 2006) (quoting *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947)) (internal quotation marks omitted).

Moreover, Wyndham is simply wrong that the FTC is announcing any "new principle" through this enforcement action. Rather, the FTC is enforcing its well-established unfairness authority to enforce Section 5 against companies that engage in practices that substantially injure consumers. *See supra* Part III.A.1. The instant action against Wyndham is simply a standard application of this authority against an entity that failed to undertake reasonable measures to protect information that it collected about consumers, which resulted in the theft of payment card data from hundreds of thousands of consumers. *See generally Neovi*, 604 F.3d 1150 (finding company engaged in unfair practices by failing to reasonably authenticate consumer information, resulting in consumer injury).

Nor would it be possible to set forth the type of particularized guidelines that Wyndham suggests would be appropriate for rulemaking. (Wyndham Mot. 11.) Data security industry standards are continually changing in response to evolving threats and new vulnerabilities and, as such, are "so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule." *Chenery Corp.*, 332 U.S. 194, 203 (1947). Moreover, industries and businesses have a variety of network structures that store or transfer different types of data, and reasonable network security will reflect the likelihood that such information will be targeted and, if so, the likely methods of attack. At its core, this is a reasonableness inquiry, which courts are well equipped to handle. *See, e.g.*, *United States v. Hanjuan Jin*, 833 F. Supp. 2d 977, 1008-09 (N.D. Ill. 2012) (evaluating, in trade secrets action, the reasonableness of Motorola's

data security, including password policies, firewalls, physical security, etc.). Thus, the FTC's authority over unfair practices as related to data security is properly exercised through case-by-case enforcement. *Chenery*, 332 U.S. at 203.

Finally, even if the FTC were announcing a "new principle," agencies are permitted to articulate principles through adjudication unless the action would constitute an abuse of discretion (such as a "sudden change of direction") or would violate the Administrative Procedure Act (such as by bypassing a pending rulemaking proceeding). *Union Flights, Inc. v. FAA*, 957 F.2d 685, 688-89 (9th Cir. 1992). The FTC has been investigating, testifying about, and providing public guidance on companies' data security obligations under the FTC Act for more than a decade, and so is not moving in a new direction through the instant action. *See supra* Argument, Part. III.A.2. Nor is there a pending rulemaking proceeding. The FTC's decision to pursue this enforcement action is therefore within its discretion.

C. The Complaint Sufficiently Alleges that Consumers Suffered Injury as a Result of Wyndham's Data Security Failures.

Neither the FTC Act nor any precedent supports Wyndham's claim that the type of injury consumers suffer as a result of the breach of payment card information does not support an unfairness allegation under15 U.S.C. § 45(n). (Wyndham Mot. 12.) The Complaint clearly alleges that consumers were injured by Wyndham's unfair data security practices:

> Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.

(Compl. ¶ 18.) This is precisely the type of "substantial injury" that the unfairness provision of the FTC Act is designed to protect against: a "small harm to a large number of people." *Neovi*, 604 F.3d at 1157-58.[8] Notwithstanding Wyndham's effort to

[8] Wyndham improperly cites a number of facts outside the four corners of the Complaint, including the consumer liability policies of major credit card brands. (Wyndham Mot. 12

distinguish the facts of *FTC v. Neovi*, its holding regarding injury is controlling here: "[O]btaining reimbursement required a substantial investment of time, trouble, aggravation, and money. . . . Regardless of whether a bank eventually restored consumers' money, the consumer suffered unavoidable injuries that could not be fully mitigated." *Neovi*, 604 F.3d at 1158 (quoting *FTC v. Neovi, Inc.*, No. 06-CV-1952-JLS, 2009 WL 56130, at *4 (S.D. Cal. Jan. 7, 2009). As the Complaint alleges, consumers suffered this type of injury as a result of Wyndham's unfair and deceptive data security practices. (Compl. ¶ 40.)

Wyndham argues that because the "risk of consumer injury posed by the theft of payment card data is . . . small, the standard of liability for failing to adequately protect such data would have to be correspondingly high." (Wyndham Mot. 13.) As a preliminary matter, the Complaint does allege substantial injury to consumers. (Compl. ¶ 40.) Moreover, the only balancing contemplated by the FTC Act is weighing the benefit to consumers of inferior information security against the injury to consumers of the resulting potential exposure of their information. *See FTC v. Inc21.com Corp.*, 745 F. Supp. 2d 975, 1004 (N.D. Cal. 2010), *aff'd*, 475 F. App'x 106 (9th Cir. 2012) (finding no countervailing benefits to unauthorized phone billing). Such a balancing test is a fact-specific inquiry and, thus, inappropriate for a motion to dismiss.

IV. THE FTC HAS ALLEGED DECEPTION BY ALL WYNDHAM ENTITIES, INCLUDING HOTELS AND RESORTS.

A. The Complaint Need Not Meet the Rule 9(b) Standard

Wyndham cursorily asserts that deception "sounds in fraud" and therefore the Complaint must satisfy the Rule 9(b) pleading requirements for this count. In support, Wyndham cites two non-binding district court cases. *FTC v. Lights of Am.*, 760 F. Supp. 2d 848, 853 (C.D. Cal. 2010); *FTC v. Ivy Capital, Inc.*, 2011 WL 2118626, at *3 (D. Nev. May 25, 2011) (following *Lights of America*). These cases are wrongly decided because a claim of deceptive practices pursuant to Section 5 of the FTC Act, "is not a claim of

n.4 and accompanying text.) Such facts are inappropriate for a motion to dismiss and, in any event, are irrelevant. *See Cervantes v. San Diego*, 5 F.3d 1273, 1274 (9th Cir. 1993).

fraud as that term is commonly understood or as contemplated by Rule 9(b)." *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1204 n.7 (10th Cir. 2005). Unlike an action for common law fraud, the Commission does not need to prove scienter, reliance, or injury to establish deception under the FTC Act. *Id. See also FTC v. Publ'g Clearing House, Inc.*, 104 F.3d 1168, 1171 (9th Cir. 1997) ("[T]he FTC is not required to show that a defendant *intended* to defraud consumers . . . ."); *FTC v. Figgie Int'l*, 994 F.2d 595, 605-06 (9th Cir. 1993) (unlike common law fraud, proof of subjective reliance by individual consumers is not required in FTC enforcement actions). Therefore, Rule 9(b) does not apply.

B. Regardless, the Complaint Meets the Rule 9(b) Standard.

Even if Rule 9(b) were applicable here, the Complaint satisfies Rule 9(b) because it provides the "the who, what, when, where, and how" of the deception. *Vess v. Ciba-Geigy Corp.*, 317 F.3d 1097, 1106 (9th Cir. 2003). The Complaint provides "specific descriptions of the representations made [and] the reasons for their falsity." *Blake v. Dierdorff*, 856 F.2d 1365, 1369 (9th Cir. 1988). To state claims that Defendants engaged in deceptive acts or practices in violation of Section 5(a) of the FTC Act, the FTC must allege that Defendants made material representations likely to mislead consumers acting reasonably under the circumstances. *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1095 (9th Cir. 1994); *Kraft, Inc. v. FTC*, 970 F.2d 311, 314 (7th Cir. 1992). Only complaints that contain "mere conclusory allegations of fraud are insufficient." *Moore v. Kayport Package Express*, 885 F.2d 531, 540 (9th Cir. 1989).

Wyndham's only explicit argument is that there cannot have been a deception because (a) the privacy policy only makes representations about information collected by Hotels and Resorts, and (b) only information collected by entities other than Hotels and Resorts was lost or stolen. (Wyndham Mot. 15.)[9] This argument is wrong legally and factually: As a legal matter, the relevant inquiry for deception is whether Wyndham misrepresented the quality of its data security; the facts of the breaches are not

[9] The FTC concedes neither the relevance nor accuracy of Wyndham's unsubstantiated assertion that no information collected by Hotels and Resorts was lost or stolen.

controlling. As a factual matter, it is simply wrong to claim that the privacy policy makes no representations about information collected by entities other than Hotels and Resorts.

First, as the Complaint states, the privacy policy expressly and impliedly makes claims about the information security measures on the Hotels and Resorts' computer network. (Compl. ¶ 21.) The Complaint also describes with specificity the information security deficiencies of that network. (*Id.* at ¶ 24.) For purposes of the deception count, the actual intrusions into the network and what data was stolen is beside the point. The Complaint need only allege that Wyndham made material representations that were false or misleading. *See Pantron I Corp.*, 33 F.3d at 1095. Here, the Complaint alleges that Wyndham's privacy policy represented, among other things, that Wyndham maintained "commercially reasonable" security (Compl. ¶ 21) and also alleges that, in fact, Wyndham did not maintain reasonable security (*id.* at ¶ 24).

Second, the Complaint pleads that Wyndham's privacy policy makes express representations about information collected by Wyndham entities *other than* Hotels and Resorts, such as information collected about *guests* at the Wyndham hotels. (Compl. ¶ 21. *See also* Wyndham Hotels and Resorts' Motion to Dismiss, Ex. 1 (ECF No. 32-1), Allen Decl., Ex. A ("Wyndham Privacy Policy") at 1) ("This policy applies to . . . *hotels of our Brands* located in the United States . . . . We recognize the importance of protecting the privacy of individual-specific (personally identifiable) information collected about *guests*, callers to our central reservation centers, visitors to our Web sites, and members participating in our Loyalty Programs (collectively '*Customers*'). . . . We safeguard our *Customers'* personal identifiable information by using industry standard practices" (emphasis added)).) Similarly, the privacy policy also makes representation about information that Hotels and Resorts controls, irrespective of how the information was collected. (Compl. ¶ 21. *See also* Wyndham Privacy Policy at 1 ("We take commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy, and that the Information is not

improperly altered or destroyed." (emphasis added)).) These provisions expressly make representations about the security of information collected from guests by Wyndham hotels.

Even if there were an express statement disclaiming these security representations, the effectiveness of such a disclaimer is a fact-specific inquiry and, as such, inappropriate for a motion to dismiss. *See FTC v. Nat'l Urological Group, Inc.*, 645 F. Supp. 2d 1167, 1189 (N.D. Ga. 2008) ("claims or net impressions communicated to reasonable consumers, is fundamentally a question of fact"). *See also FTC v. Cyberspace.Com LLC*, 453 F.3d 1196, 1200-01 (9th Cir. 2006) (affirming fact-intensive inquiry regarding net impression, and rejecting defendants' claims that "fine print notices" preclude liability). Therefore, an evaluation of the effectiveness of the disclaimer Wyndham identifies on the bottom of the fourth page (of five pages) of the privacy policy (in a paragraph that does not mention data security), is not an appropriate inquiry at this stage.

Finally, and as detailed further in its response to the Wyndham Worldwide Motion to Dismiss, the FTC alleges further that, through Hotel Management, Wyndham participated directly in the data security failures at the level of Wyndham-branded hotels, including several that compromised consumer information. (Compl. ¶ 10 ("At all relevant times, Hotel Group and Wyndham Worldwide have performed various business functions on Hotel Management's behalf, or overseen such business functions, including legal assistance and information technology and security."); *id.* at ¶ 18 ("Hotel Management controls the 'operation' of those hotels pursuant to its management agreements, including their information technology and security functions and the hiring of employees to administer the hotels' computer networks.").) Thus, even under Wyndham's incorrect and narrow "collection" construction, Wyndham has engaged in covered activities through the management activities of Hotel Management.

CONCLUSION

For the foregoing reasons, the FTC respectfully requests that the Court deny Wyndham's motion to dismiss.

Dated this 1st day of October, 2012.

s/ Kevin Moriarty

Lisa Weintraub Schifferle
Kristin Krause Cohen
Kevin H. Moriarty
Katherine E. McCarron
John A. Krebs
Andrea V. Arias
Jonathan E. Zimmerman
Federal Trade Commission
600 Pennsylvania Ave., NW Mail Stop NJ-8100
Washington, D.C. 20580

Attorneys for Plaintiff Federal Trade Commission

CERTIFICATE OF SERVICE

I hereby certify that on October 1, 2012, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to the following CM/ECF registrant:

David B. Rosenbaum, 009819
Anne M. Chapman, 025965
Osborn Maledon, P.A.
2929 North Central Avenue, Suite 2100
Phoenix, Arizona 85012-2794

Eugene F. Assaf, P.C., 449778, (Pro Hac Vice)
K. Winn Allen, 1000590, (Pro Hac Vice)
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005

Douglas H. Meal, 340971, (Pro Hac Vice)
Ropes & Gray, LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600

s/ Kevin Moriarty
Kevin H. Moriarty